EXHIBIT A

Intertrust v. MS: JCCS Claim Chart

U.S. Patent No. 6,253,193, Asserted Claim 1

	'193 Claim 1	IT Construction	MS Construction
1.	1. A method comprising:	The claim contains no requirement of a VDE.	Claim as a whole: The recited method is performed within a **VDE**. (See item #86 for Microsoft's construction of **VDE**.)
2.	receiving a digital file including music,		
3.	storing said digital file in a first **secure** memory of a first device;	secure: One or more mechanisms are employed to prevent, detect or discourage misuse of or interference with information or processes. Such mechanisms may include concealment, Tamper Resistance, Authentication and access control. Concealment means that it is difficult to read information (for example, programs may be encrypted). Tamper Resistance and Authentication are separately defined (see item #67 and item #27, respectively, below). Access control means that access to information or processes is limited on the basis of authorization. Security is not absolute, but is designed to be sufficient for a particular purpose.	secure: (1) A state in which all users of a system are guaranteed that all information, processes, and devices within the system, shall have their availability, secrecy, integrity, authenticity and nonrepudiation maintained against all of the identified threats thereto. (2) "Availability" means the property that information is accessible and usable upon demand by authorized persons, at least to the extent that no user may delete the information without authorization. (3) "Secrecy," also referred to as confidentiality, means the property that information (including computer processes) is not made available or disclosed to unauthorized persons or processes. (4) "Integrity" means the property that information has not been altered either intentionally or accidentally. (5) "Authenticity" means the property that the characteristics asserted about a person, device, program, information, or process are genuine and timely, particularly as to identity, data integrity, and origin integrity. (6) "Nonrepudiation" means the property that a sender of information cannot deny its origination and that a recipient of information cannot deny its receipt.

	'193 Claim 1	IT Construction	MS Construction
4.	storing information associated with said digital file in a **secure** database stored on said first device, said information including at least one **budget control** and	secure: see item #3 above budget: Information specifying a limitation on usage. control: Information and/or programming controlling operations on or use of resources (e.g., content) including (a) permitted, required or prevented operations, (b) the nature or extent of such operations or (c) the consequences of such operations.	secure: see item #3 above budget: (1) A unique type of "method" that specifies a decrementable numerical limitation on future **Use** (e.g., copying) of digital information and how such **Use** will be paid for, if at all. (2) A "method" is a collection of basic instructions, and information related to basic instructions, that provides context, data, requirements, and/or relationships for use in performing, and/or preparing to perform, basic instructions in relation to the operation of one or more electronic appliances. control: (1) Independent, special-purpose, **Executable**, which can execute only within a *Secure Processing Environment* (see below). (2) Each **VDE Control** is a **Component Assembly** dedicated to a particular activity (e.g., editing, modifying another **Control**, a user-defined action, etc.), particular user(s), and particular protected information, and whose satisfactory execution is necessary to *Allowing* (see below) that activity. (3) Each separate information *Access* (see below) or **Use** is independently **Controlled** by independent **VDE Control(s)**. (4) Each **VDE Control** is assembled within a *Secure Processing Environment* from independently deliverable modular components (e.g., *Load Modules* (see below) or other **Controls**), dynamically in response to an information *Access* or **Use** Request. (5) The dynamic assembly of a **Control** is directed by a "blueprint" *Record* (see below) (put in place by one or more **VDE** users) **Containing** control information identifying the exact modular code components to be

	'193 Claim 1	IT Construction	MS Construction
			assembled and executed to govern (i.e., **Control**) this particular activity on this particular information by this particular user(s). (6) Each **Control** is independently assembled, loaded and delivered vis-à-vis other **Controls**. (7) Control information and **Controls** are extensible and can be configured and modified by all users, and combined by all users with any other **VDE** control information or **Controls** (including that provided by other users), subject only to "senior" user **Controls**. (8) Users can assign control information (including alternative control information) and **Controls** to an arbitrarily fine, user-defined portion of the protected information, such as a single paragraph of a document, as opposed to being limited to file-based controls. (9) **VDE Controls** reliably limit **Use** of the protected information to only authorized activities and amounts. For the purposes of the construction of "Control," a "*Secure Processing Environment*" is defined as: A Secure Processing Environment is uniquely identifiable, self-contained, non-circumventable, and trusted by all other **VDE** nodes to protect the availability, secrecy, integrity and authenticity of all information identified in the patent application as being protected, and to guarantee that such information will be accessed and **Used** only as expressly authorized by the associated **VDE Controls**, and to guarantee that all requested reporting of and payments for protected information use will be made. A Secure Processing Environment is formed by, and requires, a Secure Processing Unit having a hardware **Tamper Resistant Barrier** encapsulating a processor and internal

	'193 Claim 1	IT Construction	MS Construction
			Secure memory. The **Tamper Resistant Barrier** prevents all unauthorized interference, removal, observation, and other Use of the information and processes within it. For the purposes of the construction of "Control," "*Allowing*" is defined as: Actively permitting an action that otherwise cannot be taken (i.e., is prohibited) by any user, process, or device. In **VDE**, an action is allowed only through execution (within a *Secure Processing Environment*) of the **VDE Control(s)** assigned to the particular action request, and satisfaction of all requirements imposed by such execution. For the purposes of the construction of "Control," "*Access*" is defined as: To satisfactorily perform the steps necessary to obtain something so that it can be **Used** in some manner (e.g., for information: copied, printed, decrypted, encrypted, saved, modified, observed, or moved, etc.). In **VDE**, access to protected information is achieved only through execution (within a *Secure Processing Environment*) of the **VDE Control(s)** assigned to the particular "access" request, satisfaction of all requirements imposed by such execution, and the **Controlled** opening of the **Secure Container Containing** the information. For the purposes of the construction of "Control," a "*Load Module*" is defined as: An **Executable**, modular unit of machine code (which may include data) suitable for loading into memory for execution by a processor. A load module is encrypted (when not within a secure processing unit) and has an **Identifier** that a calling process must provide to be able to use the load module. A load module is combinable with other load modules,

	'193 Claim 1	IT Construction	MS Construction
			and associated data, to form **Executable Component Assemblies.** A load module can execute only in a **VDE Protected Processing Environment.** Library routines are not load modules and dynamic link libraries are not load modules. For the purposes of the construction of "Control," a "*Record*" is defined as: A data structure that is a collection of fields (elements), each with its own name and type. Unlike an array, whose elements are accessed using an index, the elements of a record are accessed by name. A record can be accessed as a collective unit of elements, or the elements can be accessed individually.
5.	at least one **copy control,**	copy: To reproduce. The reproduction must be usable, may incorporate all of the original item or only some of it, and may involve some changes to the item as long as the essential nature of the content remains unchanged. control: see item #4 above	copy: (1) To reproduce all of a *Digital File* (see below) or other complete physical block of data from one location on a storage medium to another location on the same or different storage medium, leaving the original block of data unchanged, such that two distinct and independent objects exist. (2) Although the layout of the data values in physical storage may differ from the original, the resulting "copy" is logically indistinguishable from the original. (3) The resulting "copy" may or may not be encrypted, ephemeral, usable, or accessible. For the purposes of the construction of "Copy," a "*Digital File*" is defined as: A named, static unit of storage allocated by a "file system" and **Containing** digital information. A digital file enables any application using the "file system" to randomly access its contents and to distinguish it by name from every other such unit. A copy of a digital file is a separate digital file. A "file system" is the portion of the operating system

	'193 Claim 1	IT Construction	MS Construction
			that translates requests made by application programs for operations on "files" into low-level tasks that can control storage devices such as disk drives. control: see item #4 above
6.	said at least one **budget control** including *a budget specifying the number of copies which can be made of said digital file*;	budget: see item #4 above control: see item #4 above a budget specifying the number of copies which can be made of said digital file: Normal English, incorporating the separately defined terms: a Budget stating the number of copies that can be made of the digital file referred to earlier in the claim.	budget: see item #4 above control: see item #4 above a budget specifying the number of copies which can be made of said digital file: A **Budget** explicitly stating the total number of copies (whether or not decrypted, long-lived, or accessible) that (since creation of the **Budget**) are authorized to be made of the *Digital File* by any and all users, devices, and processes. No process, user, or device is able to make another copy of the *Digital File* once this number of copies has been made. For the purposes of the construction of this phrase, "*Digital File*" is defined as set forth in item #5, above.
7.	and said at least one **copy control** *controlling the copies made of said digital file*;	copy: see item #5 above control: see item #4 above controlling: Normal English: exercising authoritative or dominating influence over; directing. controlling the copies made of said digital file: The nature of this operation is further defined in later claim elements. In context, the copy control determines the conditions under which a digital file may be Copied and the copied file stored on a second device.	copy: see item #5 above control: see item #4 above controlling: (1) Reliably defining and enforcing the conditions and requirements under which an action that otherwise cannot be taken, will be *Allowed*, and the manner in which it may occur. Absent verified satisfaction of those conditions and requirements, the action cannot be taken by any user, process or device. (2) In **VDE**, an action is **Controlled** through execution of the applicable **VDE Control(s)** within a **VDE** *Secure Processing Environment*. (3) More specifically, in **VDE**, **Controlling** is effected by use of **VDE Controls**, **VDE Secure Containers**, and **VDE** foundation

	'193 Claim 1	IT Construction	MS Construction
			(including **VDE** *Secure Processing Environment*, "object registration," and other mechanisms for allegedly individually ensuring that specific **Controls** are enforced vis-à-vis specific objects (and their content at an arbitrary granular level) and specific "users"). For the purposes of the construction of "Control (v.)" et al, "*Allowed*" and "*Secure Processing Environment*" are defined as set forth in item #4, above. controlling the copies made of said digital file: **Controlling Uses** of and *Accesses* to all copies of the *Digital File*, by all users, processes, and devices, by executing each of the recited "at least one" **Copy Control(s)** within **VDE** *Secure Processing Environment(s)*. Each **Control** governs **(Controls)** only one action, which action may or may not differ among the different "at least one" **Controls**. All **Uses** and *Accesses* are prohibited and incapable of occurring except to the extent *Allowed* by the "at least one" **Copy Control(s)**. For the purposes of the construction of this phrase, "*Secure Processing Environment,*" "*Access*" and "*Allowed*" are defined as set forth in item #4, above.

	'193 Claim 1	IT Construction	MS Construction
8.	determining whether said digital file may be **copied** and stored on a second device based on at least said **copy control**;	copied (copy): see item #5 above control: see item #4 above	copied (copy): see item #5 above control: see item #4 above
9.	if said **copy control** allows at least a portion of said digital file to be **copied** and stored on a second device,	copied (copy): see item #5 above control: see item #4 above	copied (copy): see item #5 above control: see item #4 above
10.	**copying** at least a portion of said digital file;	copying (copy): see item #5 above	copying (copy): see item #5 above
11.	transferring at least a portion of said digital file to a second device including a memory and an audio and/or video output;		
12.	storing said digital file in said memory of said second device; and		
13.	including playing said music through said audio output.		

U.S. Patent No. 6,253,193, Asserted Claim 11

	'193 Claim 11	IT Construction	MS Construction
14.	11. A method comprising:	The claim contains no requirement of a VDE.	Claim as a whole: The recited method is performed within a **VDE**. (See item #86 for Microsoft's construction of **VDE**.)
15.	receiving a digital file;		
16.	storing said digital file in a first **secure** memory of a first device;	secure: see item #3 above	secure: see item #3 above
17.	storing information associated with said digital file in a **secure** database stored on said first device, said information including a first **control**;	secure: see item #3 above control: see item #4 above	secure: see item #3 above control: see item #4 above
18.	determining whether said digital file may be **copied** and stored on a second device based on said first **control**, said determining step including identifying said second device and determining whether,	copied (copy): see item #5 above control: see item #4 above	copied (copy): see item #5 above control: see item #4 above
19.	said first **control** allows transfer of said **copied** file to said second device, said determination based at least in part on the features present at the device to which said **copied** file is to be transferred;	control: see item #4 above copied (copy): see item #5 above	control: see item #4 above copied (copy): see item #5 above

	'193 Claim 11	IT Construction	MS Construction
20.	if said first **control** allows at least a portion of said digital file to be **copied** and stored on a second device,	control: see item #4 above copied (copy): see item #5 above	control: see item #4 above copied (copy): see item #5 above
21.	**copying** at least a portion of said digital file;	copying (copy): see item #5 above	copying (copy): see item #5 above
22.	transferring at least a portion of said digital file to a second device including a memory and an audio and/or video output;		
23.	storing said digital file in said memory of said second device; and		
24.	rendering said digital file through said output.		

U.S. Patent No. 6,253,193, Asserted Claim 15

	'193 Claim 15	IT Construction	MS Construction
25.	15. A method comprising:	The claim contains no requirement of a VDE.	Claim as a whole: The recited method is performed within a **VDE**. (See item #93 for Microsoft's construction of **VDE**.)
26.	receiving a digital file;		
27.	an **authentication** step comprising:	authentication: Identifying (e.g., a person, device, organization, document, file, etc.). Includes uniquely identifying or identifying as a member of a group.	authentication: To establish that the following asserted characteristics of something (e.g., a person, device, organization, document, file, etc.) are genuine: its identity, its data integrity, (i.e., it has not been altered) and its origin integrity (i.e., its source and time of origination).
28.	accessing at least one **identifier** associated with a first device or with a user of said first device; and	identifier: Information used to identify something or someone (e.g., a password). In this definition, "identify" means to establish the identity of or to ascertain the origin, nature, or definitive characteristics of; includes identifying as an individual or as a member of a group.	identifier: Any text string used as a label naming an individual instance of what it *Identifies* (see below) For the purpose of the construction of "Identifier," *"Identify"* is defined as: To establish as being a particular instance of a person or thing.
29.	determining whether said **identifier** is associated with a device and/or user authorized to store said digital file;	identifier: see item #28 above	identifier: see item #28 above
30.	storing said digital file in a first **secure** memory of said first device, but only if said device and/or user is so authorized, but not proceeding with said storing if said device and/or user is not authorized;	secure: see item #3 above	secure: see item #3 above
31.	storing information associated with said digital file in a **secure** database stored on said first	secure: see item #3 above control: see item #4 above	secure: see item #3 above control: see item #4 above

	'193 Claim 15	IT Construction	MS Construction
	device, said information including at least one **control**;		
32.	determining whether said digital file may be **copied** and stored on a second device based on said at least one **control**;	copied (copy): see item #5 above control: see item #4 above	copied (copy): see item #5 above control: see item #4 above
33.	if said at least one **control** allows at least a portion of said digital file to be **copied** and stored on a second device,	control: see item #4 above copied (copy): see item #5 above	control: see item #4 above copied (copy): see item #5 above
34.	**copying** at least a portion of said digital file;	copying (copy): see item #5 above	copying (copy): see item #5 above
35.	transferring at least a portion of said digital file to a second device including a memory and an audio and/or video output;		
36.	storing said digital file in said memory of said second device; and		
37.	rendering said digital file through said output.		

U.S. Patent No. 6,253,193, Asserted Claim 19

	'193 Claim 19	IT Construction	MS Construction
38.	19. A method comprising:	The claim contains no requirement of a VDE.	Claim as a whole: The recited method is performed within a **VDE**. (See item #86 for Microsoft's construction of **VDE**.)
39.	receiving a digital file at a first device;		
40.	establishing communication between said first device and a **clearinghouse** located at a location remote from said first device;	clearinghouse: A provider of financial and/or administrative services for a number of entities; or an entity responsible for the collection, maintenance, and/or distribution of materials, information, licenses, etc.	clearinghouse: (1) A computer system that provides intermediate storing and forwarding services for both content and audit information, and which two or more parties trust to provide its services independently because it is operated under constraint of **VDE** security. (2) "Audit information" means all information created, stored, or reported in connection with an "auditing" process. "Auditing" means tracking, metering and reporting the usage of particular information or a particular appliance.
41.	said first device obtaining authorization information including a key from said **clearinghouse**;	clearinghouse: see item #40 above	clearinghouse: see item #40 above
42.	said first device using said authorization information to gain access to or make at least one **use** of said first digital file, including using said key to decrypt at least a portion of said first digital file; and	use: Normal English: to put into service or apply for a purpose, to employ.	use: (1) To use information is to perform some action on it or with it (e.g., copying, printing, decrypting, encrypting, saving, modifying, observing, or moving, etc.). (2) In **VDE**, information **Use** is *Allowed* only through execution of the applicable **VDE Control(s)** and satisfaction of all requirements imposed by such execution. For the purposes of the construction of "Use," "*Allowed*" is defined as set forth in item #4, above.
43.	receiving a first **control** from said **clearinghouse** at said first device;	control: see item #4 above clearinghouse: see item #40 above	control: see item #4 above clearinghouse: see item #40 above

	'193 Claim 19	IT Construction	MS Construction
44.	storing said first digital file in a memory of said first device;		
45.	using said first **control** to determine whether said first digital file may be **copied** and stored on a second device;	control: see item #4 above copied (copy): see item #5 above	control: see item #4 above copied (copy): see item #5 above
46.	if said first **control** allows at least a portion of said first digital file to be **copied** and stored on a second device,	control: see item #4 above copied (copy): see item #5 above	control: see item #4 above copied (copy): see item #5 above
47.	**copying** at least a portion of said first digital file;	copying (copy): see item #5 above	copying (copy): see item #5 above
48.	transferring at least a portion of said first digital file to a second device including a memory and an audio and/or video output;		
49.	storing said first digital file portion in said memory of said second device; and		
50.	rendering said first digital file portion through said output.		

U.S. Patent No. 6,185,683, Asserted Claim 2

	'683 Claim 2	IT Construction	MS Construction
51.	2. A system including:	The claim contains no requirement of a VDE.	Claim as a Whole: The "system" is a **VDE**. (See item #86 for Microsoft's construction of **VDE**.)
52.	a first apparatus including,		
53.	user **controls**,	control: see item #4 above	control: see item #4 above
54.	a communications port,		
55.	a processor,		
56.	a memory storing:		
57.	a first **secure container**	secure container: A container that is Secure. In this definition, "container" means a digital file containing linked and/or embedded items.	secure container: (1) A **VDE Secure Container** is a self-contained, self-protecting data structure which (a) encapsulates information of arbitrary size, type, format, and organization, including other, nested, containers, (b) cryptographically protects that information from all unauthorized *Access* and **Use**, (c) provides encrypted storage management functions for that information, such as hiding the physical storage location(s) of its protected contents, (d) permits the association of itself or its contents with **Controls** and control information governing **(Controlling)** *Access* to and **Use** thereof, and (e) prevents such **Use** or *Access* (as opposed to merely preventing decryption) until it is "opened." (2) A **Secure Container** can be opened only as expressly *Allowed* by the associated **VDE Control(s)**, only within a *Secure Processing Environment*, and only through decryption of its encrypted header. (3) A **Secure Container** is not directly accessible to any non-**VDE** or user calling process. All such calls are intercepted by **VDE**. (4) The creator of a **Secure Container** can assign (or allow others to assign) control information to any arbitrary portion of a **Secure Container**'s contents, or to an empty **Secure Container** (to govern

	'683 Claim 2	IT Construction	MS Construction
			(**Control**) the later addition of contents to the container, and *Access* to or **Use** of those contents). (5) A container is not a **Secure Container** merely because its contents are encrypted and signed. A **Secure Container** is itself **Secure**. (6) All **VDE**-protected information (including protected content, information about content usage, content-control information, **Controls**, and *Load Modules*) is encapsulated within a **Secure Container** whenever stored outside a *Secure Processing Environment* or secure database. For the purposes of the construction of "Secure Container," "*Secure Processing Environment*," "*Load Module*," "*Access*" and "*Allow*" are defined as set forth in item #4, above.
58.	**containing** a governed item,	containing: Normal English: having within or holding. In the context of an element contained within a data structure (e.g., a secure container), the contained element may be either directly within the container or the container may hold a reference indicating where the element may be found.	containing: Physically (directly) storing within, as opposed to addressing (i.e., referring to something by the explicitly identified location where it is stored, without directly storing it).
59.	the first **secure container** governed item being at least in part encrypted; the first **secure container** having been received from a second apparatus;	secure container: see item #57 above	secure container: see item #57 above

	'683 Claim 2	IT Construction	MS Construction
60.	a first **secure container** rule at least in part governing an **aspect** of access to or **use** of said first **secure container** governed item, the first **secure container** rule, the first **secure container** rule having been received from a third apparatus different from said second apparatus; and	secure container: see item #57 above aspect: Feature, element, property or state. use: see item #42 above	secure container: see item #57 above aspect: An aspect of an environment is a persistent element or property of that environment that can be used to distinguish it from other environments. use: see item #42 above
61.	hardware or software used for receiving and opening **secure containers**, said **secure containers** each including the capacity to **contain** a governed item, a **secure container** rule being associated with each of said **secure containers**;	secure container: see item #57 above contain (containing): see item #58 above	secure container: see item #57 above contain (containing): see item #58 above
62.	a **protected processing environment** at least in part protecting information **contained** in said **protected processing environment** from tampering by a user of said first apparatus,	protected processing environment: An environment in which processing and/or data is at least in part protected from tampering. The level of protection can vary, depending on the threat. In this definition, "environment" means capabilities available to a program running on a computer or other device or to the user of a computer or other device. Depending on the context, the environment may be in a single device (e.g., a personal computer) or may be spread among multiple	protected processing environment: (1) A uniquely identifiable, self-contained computing base trusted by all **VDE** nodes to protect the availability, secrecy, integrity and authenticity of all information identified in the February, 1995, patent application as being protected, and to guarantee that such information will be *Accessed* and **Used** only as expressly authorized by **VDE Controls**. (2) At most **VDE** nodes, the **Protected Processing Environment** is a *Secure Processing Environment* which is formed by, and requires, a

	'683 Claim 2	IT Construction	MS Construction
		devices (e.g., a network). contained (containing): see item #58 above	hardware **Tamper Resistant Barrier** encapsulating a special-purpose Secure Processing Unit having a processor and internal secure memory. "Encapsulated" means hidden within an object so that it is not directly accessible but rather is accessible only through the object's restrictive interface. (3) The **Tamper Resistant Barrier** prevents all unauthorized (intentional or accidental) interference, removal, observation, and use of the information and processes within it, by all parties (including all users of the device in which the **Protected Processing Environment** resides), except as expressly authorized by **VDE Controls**. (4) A **Protected Processing Environment** is under **Control** of **Controls** and control information provided by one or more parties, rather than being under **Control** of the appliance's users or programs. (5) Where a **VDE** node is an established financial **Clearinghouse**, or other such facility employing physical facility and user-identity **Authentication** security procedures trusted by all **VDE** nodes, and the **VDE** node does not *Access* or **Use** **VDE**-protected information, or assign **VDE** control information, then the **Protected Processing Environment** at that **VDE** node may instead be formed by a general-purpose CPU that executes all **VDE** "security" processes in protected (privileged) mode. (6) A **Protected Processing Environment** requires more than just verifying the integrity of **Digitally Signed Executable** programming prior to execution of the programming; or concealment of the program, associated data, and execution of the program code; or use of a password as its protection

	'683 Claim 2	IT Construction	MS Construction
			mechanism. For the purposes of the construction of "Protected Processing Environment," "*Secure Processing Environment*" and "*Access*" are defined as set forth in item #4, above. contained (containing): see item #58 above
63.	said **protected processing environment** including hardware or software used for applying said first **secure container** rule and a second **secure container** rule in combination to at least in part govern at least one **aspect** of access to or **use** of a governed item **contained** in a **secure container**; and	protected processing environment: see item #62 above secure container: see item #57 above aspect: see item #60 above use: see item #42 above contained (containing): see item #58 above	protected processing environment: see item #62 above secure container: see item #57 above aspect: see item #60 above use: see item #42 above contained (containing): see item #58 above
64.	hardware or software used for transmission of **secure containers** to other apparatuses or for the receipt of **secure containers** from other apparatuses.	secure container: see item #57 above	secure container: see item #57 above

U.S. Patent No. 6,157,721, Asserted Claim 1

	'721 Claim 1	IT Construction	MS Construction
65.	1. A security method comprising:	The claim contains no requirement of a VDE.	Claim as a whole: The recited method is performed within a **VDE**. (See item #86 for Microsoft's construction of **VDE**.)
66.	**digitally signing** a first load module with a first **digital signature designating** the first load module for **use** by a first **device class**;	digital signature: A digital value, verifiable with a key, that can be used to determine the source and/or integrity of a signed item (e.g., a file, program, etc.). Digitally signing is the process of creating a digital signature. designating: Normal English: indicating, specifying, pointing out or characterizing. use: see item #42 above device class: A group of devices which share at least one attribute.	digitally signing: (1) Creating a **Digital Signature** using a secret *Key* (see below). (2) In symmetric key cryptography, a "secret key" is a *Key* that is known only to the sender and recipient. In asymmetric key cryptography, a "secret key" is the private *Key* of a public/private key pair, in which the two keys are related uniquely by a predetermined mathematical relationship such that it is computationally infeasible to determine one from the other. For the purposes of the construction of "Digital Signing," a "*Key*" is defined as: A bit sequence used and needed by a cryptographic algorithm to encrypt a block of plain text or to decrypt a block of cipher text. A key is different from a key seed or other information from which the actual encryption and/or decryption key is constructed, **Derived**, or otherwise identified. In symmetric key cryptography, the same key is used for both encryption and decryption. In asymmetric or "public key" cryptography, two related keys are used; a block of text encrypted by one of the two keys (e.g., the "public key") can be decrypted only by the corresponding key (e.g., the "private key"). digital signature: A computationally unforgeable string of characters (e.g., bits) generated by a cryptographic operation on a block of data using some secret. The string can be generated only by an entity that knows the secret, and hence provides

	'721 Claim 1	IT Construction	MS Construction
			evidence that the entity must have generated it. designating: Designating something for a particular Use means specifying it for and restricting it to that Use. use: see item #42 above device class: The generic name for a group of device types. For example, all display stations belong to the same device class. A device class is different from a device type. A device type is composed of all devices that share a common model number or family (e.g. IBM 4331 printers).
67.	***digitally signing*** *a second load module with a second* ***digital signature*** *different from the first* ***digital signature****, the second* ***digital signature*** ***designating*** *the second load module for* ***use*** *by a second* ***device class*** *having at least one of* ***tamper resistance*** *and security level different from the at least one of* ***tamper resistance*** *and security level of the first* ***device class****;*	digital signature: see item #66 above designating: see item #66 above use: see item #42 above device class: see item #66 above tamper resistance: Making tampering more difficult and/or allowing detection of tampering. In this definition, "tampering" means using (e.g., observing or altering) in any unauthorized manner, or interfering with authorized use. digitally signing a second load module with a second digital signature different from the first digital signature, the second digital signature designating the second load module for use by a second device class having at least one of tamper resistance and security level different from the at least one of tamper resistance and security level of the first device class: Normal English, incorporating the separately defined terms: generating a Digital Signature	digital signature: see item #66 above designating: see item #66 above use: see item #42 above device class: see item #66 above tamper resistance: The ability of a **Tamper Resistant Barrier** to prevent *Access*, observation, and interference with information or processing encapsulated by the barrier. For the purposes of the construction of "Tamper Resistance," "*Tamper/Tampering*" is defined as: Using (e.g., observing or altering) in any unauthorized manner, or interfering with authorized use. For the purposes of the construction of "Tamper Resistance," "*Access*" is defined as set forth in item #4, above. digitally signing a second load module with a second digital signature different from the first digital signature, the second digital signature designating the second load module for use by a second device

	'721 Claim 1	IT Construction	MS Construction
		for the second load module, the Digital Signature Designating that the second load module is for use by a second Device Class. This element further requires that the second Device Class have a different Tamper Resistance or security level than the first Device Class.	class having at least one of tamper resistance and security level different from the at least one of tamper resistance and security level of the first device class: (1) **Digitally Signing** a different ("second") *Load Module* by using a different ("second") **Digital Signature** as the signature *Key*, which signing indicates to any and all devices in the second **Device Class** that the signor authorized and restricted this *Load Module* for **Use** by that device. (2) No **VDE** device can perform any execution of any *Load Module* without such authorization. The method ensures that the *Load Module* cannot execute in a particular **Device Class** and ensures that no device in that **Device Class** has the *Key(s)* necessary to verify the **Digital Signature**. (3) All devices in the first **Device Class** have the same persistent (not just occasional) and identified level of **Tamper Resistance** and the same persistent and identified level of security. All devices in the second **Device Class** have the same persistent and identified level of **Tamper Resistance** and same persistent and identified level of security. (4) The identified level of **Tamper Resistance** or identified level of security (or both) for the first **Device Class**, is greater than or less than the identified level of **Tamper Resistance** or identified level of security for the second **Device Class**. For the purposes of the construction of this phrase, a "*Load Module*" is defined as set forth in item #4 and "*Key*" is defined as set forth in item #66, above.

	'721 Claim 1	IT Construction	MS Construction
68.	distributing the first load module for **use** by at least one device in the first **device class**; and	use: see item #42 above device class: see item #66 above	use: see item #42 above device class: see item #66 above
69.	distributing the second load module for **use** by at least one device in the second **device class**.	use: see item #42 above device class: see item #66 above	use: see item #42 above device class: see item #66 above

U.S. Patent No. 6,157,721, Asserted Claim 34

	'721 Claim 34	IT Construction	MS Construction
70.	34. A **protected processing environment** comprising:	The claim contains no requirement of a VDE protected processing environment: see item #62 above "Protected processing environment" appears in the preamble of this claim. InterTrust reserves the right to assert that it should not be defined, other than as requiring the individual claim elements.	Claim as a Whole: The "**Protected Processing Environment**" is part of and within **VDE**. (See item #86 for Microsoft's construction of **VDE**.) protected processing environment: see item #62 above
71.	a first **tamper resistant barrier** having a first security level,	tamper resistant barrier: Hardware and/or software that provides Tamper Resistance.	tamper resistant barrier: (1) An active device that encapsulates and separates a **Protected Processing Environment** from the rest of the world. (2) It prevents information and processes within the **Protected Processing Environment** from being observed, interfered with, and leaving except under appropriate conditions ensuring security. (3) It also **Controls** external access to the encapsulated **Secure** resources, processes and information. (4) A **Tamper Resistant Barrier** is capable of destroying protected information in response to *Tampering* attempts. For the purposes of the construction of "Tamper Resistant Barrier," "*Tamper/Tampering*" is defined as set forth in item #67, above.
72.	a first **secure** execution space, and	secure: see item #3 above	secure: see item #3 above

	'721 Claim 34	IT Construction	MS Construction
73.	at least one arrangement within the first **tamper resistant barrier** that prevents the first **secure** execution space from executing the same **executable** accessed by a second **secure** execution space having a second **tamper resistant barrier** with a second security level different from the first security level.	tamper resistant barrier: see item #71 above secure: see item #3 above executable: A computer program that can be run, directly or through interpretation.	tamper resistant barrier: see item #71 above secure: see item #3 above executable: A cohesive series of machine code instructions in a format that can be loaded into memory and run (executed) by a connected processor.

U.S. Patent No. 5,920,861, Asserted Claim 58

	'861 Claim 58	IT Construction	MS Construction
74.	58. A method of creating a first **secure container**, said method including the following steps;	The claim contains no requirement of a VDE. secure container: see item #57 above	Claim as a whole: The recited method is performed within a **VDE**. (See item #86 for Microsoft's construction of **VDE**.) secure container: see item #57 above
75.	accessing a descriptive data structure, said descriptive data structure including or addressing		
76.	organization information at least in part describing a required or desired organization of a content section of said first **secure container**, and	secure container: see item #57 above	secure container: see item #57 above
77.	metadata information at least in part specifying at least one step required or desired in creation of said first **secure container**;	secure container: see item #57 above	secure container: see item #57 above
78.	using said descriptive data structure to organize said first **secure container** contents;	secure container: see item #57 above	secure container: see item #57 above
79.	using said metadata information to at least in part determine specific information required to be included in said first **secure container** contents; and	secure container: see item #57 above	secure container: see item #57 above

	'861 Claim 58	IT Construction	MS Construction
80.	generating or identifying at least one rule designed to **control** at least one **aspect** of access to or **use** of at least a portion of said first **secure container** contents.	control (controlling): see item #7 above aspect: see item #60 above use: see item #42 above secure container: see item #57 above	control (controlling): see item #7 above aspect: see item #60 above use: see item #42 above secure container: see item #57 above

U.S. Patent No. 5,982,891, Asserted Claim: 1

	'891 Claim 1	IT Construction	MS Construction
81.	1. A method for using at least one resource processed in a **secure** operating environment at a first appliance, said method comprising:	The claim contains no requirement of a VDE. secure: see item #3 above	Claim as a whole: The recited method is performed within a **VDE**. (See item #86 for Microsoft's construction of **VDE**.) secure: see item #3 above
82.	**securely** receiving a first entity's **control** at said first appliance, said first entity being located remotely from said operating environment and said first appliance;	securely (secure): see item #3 above control: see item #4 above	securely (secure): see item #3 above control: see item #4 above
83.	**securely** receiving a second entity's **control** at said first appliance, said second entity being located remotely from said operating environment and said first appliance, said second entity being different from said first entity; and	securely (secure): see item #3 above control: see item #4 above	securely (secure): see item #3 above control: see item #4 above
84.	**securely** processing a data item at said first appliance, using at least one resource, including	securely (secure): see item #3 above	securely (secure): see item #3 above
85.	***securely** applying, at said first appliance through **use** of said at least one resource said first entity's **control** and said second entity's **control** to govern **use** of said data item.*	securely (secure): see item #3 above use: see item #42 above control: see item #4 above securely applying, at said first appliance through use of said at least one resource said first entity's control and said second entity's control to govern use of said data item: Normal English, incorporating the separately defined terms: the first entity's Control	securely (secure): see item #3 above use: see item #42 above control: see item #4 above securely applying, at said first appliance through use of said at least one resource said first entity's control and said second entity's control to govern use of said data item: (1) Processing the resource (component part of a first appliance's Secure

	'891 Claim 1	IT Construction	MS Construction
		and the second entity's Control are Securely applied to govern Use of the data item, the act of Securely applying involving use of the resource.	Operating Environment) within the Secure Operating Environment's special-purpose Secure Processing Unit (SPU) to execute the first **Control** and second **Control** in combination within the SPU. (2) This execution of these **Controls** governs (**Controls**) all **Use** of the data item by all users, processes, and devices. (3) The processing of the resource and execution of the **Controls** cannot be observed from outside the SPU and is performed only after the integrity of the resource and **Controls** is cryptographically verified. (4) A Secure Processing Unit is a special-purpose unit isolated from the rest of the world in which a hardware **Tamper Resistant Barrier** encapsulates a processor and internal **Secure** memory. (5) The processor cryptographically verifies the integrity of all code loaded from the **Secure** memory prior to execution, executes only the code that the processor has authenticated for its **Use**, and is otherwise **Secure**.

Patent No. 5,892,900, Asserted Claim: 155

	'900 Claim 155	IT Construction	MS Construction
86.	155. A **virtual distribution environment** comprising	Virtual Distribution Evironment: This term is contained in the preamble of the claim and should not be defined, other than as requiring the individual claim elements. Without waiving its position that no separate definition is required, if required to propose such a definition, InterTrust proposes the following: secure, distributed electronic transaction management and rights protection system for controlling the distribution and/or other usage of electronically provided and/or stored information.	Claim as a Whole: The "virtual distribution environment" is **VDE**. Virtual Distribution Environment: (1) Data Security and Commerce World: InterTrust's February 13, 1995, patent application described as its "invention" a **Virtual Distribution Environment** ("VDE invention") for securing, administering, and auditing all security and commerce digital information within its multi-node world (community). **VDE** guarantees to all **VDE** "participants" identified in the patent application that it will limit all *Access* to and **Use** (i.e., interaction) of such information to authorized activities and amounts, will ensure any requested reporting of and payment for such **Use**, and will maintain the availability, secrecy, integrity, non-repudiation and authenticity of all such information present at any of its nodes (including protected content, information about content usage, and content **Controls**.). **VDE** is **Secure** against at least the threats identified in the Feburary 1995, patent application to this availability (no user may delete the information without authorization), secrecy (neither available nor disclosed to unauthorized persons or processes), integrity (neither intentional nor accidental alteration), non-repudiation (neither the receiver can disavow the receipt of a message nor can the sender disavow the origination of that message) and authenticity (asserted characteristics are genuine). **VDE** further provides and requires the components and capabilities described below. Anything less than or different than this is not **VDE** or the described "invention."

	'900 Claim 155	IT Construction	MS Construction
			(2) Secure Processing Environment: At each node where **VDE**-protected information is *Accessed*, **Used**, or assigned control information, **VDE** requires a *Secure Processing Environment* (as set forth in item #6). (3) VDE Controls: **VDE Allows** *Access* to or **Use** of protected information and processes only through execution of (and satisfaction of the requirements imposed by) **VDE Control(s)**. (4) VDE Secure Container: See construction of **Secure Container** (see item #57). (5) Non-Circumventable: **VDE** is non-circumventable (sequestered). It intercepts all attempts by any and all users, processes, and devices, to *Access* or **Use**, such as observing, interfering with, or removing) protected information, and prevents all such attempts other than as allowed by execution of (and satisfaction of all requirements imposed by) associated **VDE Controls** within *Secure Processing Environment(s)*. (6) Peer to Peer: **VDE** is peer-to-peer. Each **VDE** node has the innate ability to perform any role identified in the patent application (e.g., end user, content packager, distributor, **Clearinghouse**, etc.), and can protect information flowing in any direction between any nodes. **VDE** is not client-server. It does not pre-designate and restrict one or more nodes to act solely as a "server" (a provider of information (e.g., authored content, control information, etc.) to other nodes) or "client" (a requestor of such information). All types of protected-content transactions can proceed without requiring interaction with any server.

	'900 Claim 155	IT Construction	MS Construction
			(7) Comprehensive Range of Functions: **VDE** comprehensively governs (**Controls**) all security and commerce activities identified in the patent application, including (a) metering, budgeting, monitoring, reporting, and auditing information usage, (b) billing and paying for information usage, and (c) negotiating, signing and enforcing contracts that establish users' rights to *Access* or **Use** information. (8) User-Configurable: The specific protections governing (**Controlling**) specific **VDE**-protected information are specified, modified, and negotiated by **VDE**'s users. For example, **VDE** enables a consumer to place limits on the nature of content that may be *Accessed* at her node (e.g., no R-rated material) or the amount of money she can spend on viewing certain content, both subject only to other users' senior **Controls**. (9) General Purpose; Universal: **VDE** is universal as opposed to being limited to or requiring any particular type of appliance, information, or commerce model. It is a single, unified standard and environment within which an unlimited range of electronic rights protection, data security, electronic currency, and banking applications can run. (10) Flexible: **VDE** is more flexible than traditional information security and commerce systems. For example, **VDE** allows consumers to pay for only the user-defined portion of information that the user actually uses, and to pay only in proportion to any quantifiable **VDE** event (e.g., for only the number of paragraphs displayed from a book), and allows editing the content in **VDE** containers while maintaining its security.

	'900 Claim 155	IT Construction	MS Construction
			For the purposes of the construction of "VDE," "*Secure Processing Environment*" and "*Access*" are defined as set forth in item #4, above.
87.	a first **host processing environment** comprising	host processing environment: This term is explicitly defined in the claim and therefore needs no additional definition. It consists of those elements listed in the claim. Without waiving its position that no separate definition is required, if required to propose such a definition, InterTrust proposes the following: a Protected Processing Environment incorporating software-based security.	host processing environment: (1) A processing environment within a **VDE** node which is not a *Secure Processing Environment.* (2) A "host processing environment" may either be "secure" or "not secure." (3) A "secure host processing environment" is a self-contained **Protected Processing Environment**, formed by loaded, **Executable** programming executing on a general purpose CPU (not a Secure Processing Unit) running in protected (privileged) mode. (4) A "non-secure host processing environment" is formed by loaded, **Executable** programming executing on a general purpose CPU (not a Secure Processing Unit) running in user mode. For the purposes of the construction of "Host Processing Environment," a "*Secure Processing Environment*" is defined as set forth in item #4, above.
88.	a central processing unit;		
89.	main memory operatively connected to said central processing unit;		
90.	mass storage operatively connected to said central processing unit and said main memory;		

	'900 Claim 155	IT Construction	MS Construction
91.	said mass storage storing tamper resistant software designed to be loaded into said main memory and executed by said central processing unit, said tamper resistant software comprising:		
92.	machine check programming which ***derives information from one or more aspects of said host processing environment,***	derives: Normal English: obtains, receives or arrives at through a process of reasoning or deduction. In the context of computer operations, the "process of reasoning or deduction" constitutes operations carried out by the computer. aspect: see item #60 above host processing environment: see item #87 above derives information from one or more aspects of said host processing environment: Normal English, incorporating the separately defined terms: Derives (including creates) information based on at least one Aspect of the previously referred to Host Processing Environment.	derives: To retrieve from a specified source. aspect: see item #60 above host processing environment: see item #87 above derives information from one or more aspects of said host processing environment: (1) **Deriving** from the **Host Processing Environment** hardware one or more values that uniquely and persistently identify the **Host Processing Environment** and distinguish it from other **Host Processing Environments.** (2) The "one or more aspects of said host processing environment" are persistent elements or properties of the **Host Processing Environment** itself that are capable of being used to distinguish it from other environments, as opposed to, e.g., data or programs stored within the mass storage or main memory, or processes executing within the **Host Processing Environment.**
93.	one or more storage locations storing said information;		

	'900 Claim 155	IT Construction	MS Construction
94.	integrity programming which causes said machine check programming to **derive** said information, **compares** said information to information previously stored in said one or more storage locations, and	derive: see item #92 above compares: Normal English: examines for the purpose of noting similarities and differences. "Comparison" refers to the act of comparing.	derive: see item #92 above compares: A processor operation that evaluates two quantities and sets one of three flag conditions as a result of the comparison – greater than, less than, or equal to.
95.	generates an indication based on the result of said **comparison**; and	comparison (compares): see item #94 above	comparison (compares): see item #94 above
96.	programming which takes one or more actions based on the state of said indication;		
97.	said one or more actions including at least temporarily halting further processing.		

U.S. Patent No. 5,917,912, Asserted Claim: 8

	'912 Claim 8	IT Construction	MS Construction
98.	8. A process comprising the following steps:	The claim contains no requirement of a VDE.	Claim as a whole: The recited method is performed within a **VDE**. (See item #93 for Microsoft's construction of **VDE**.)
99.	accessing a first record **containing** information directly or indirectly identifying one or more elements of a first **component assembly,**	containing: see item #58 above component assembly: Components are code and/or data elements that are independently deliverable. A Component Assembly is two or more components associated together. Component Assemblies are utilized to perform operating system and/or applications tasks.	containing: see item #58 above component assembly: (1) A cohesive **Executable** component created by a channel which binds or links together two or more independently deliverable *Load Modules*, and associated data. (2) A **Component Assembly** is assembled, and executes, only within a **VDE** *Secure Processing Environment*. (3) A **Component Assembly** is assembled dynamically in response to, and to service, a particular content-related activity (e.g., a particular **Use** request). (4) Each **VDE Component Assembly** is assigned and dedicated to a particular activity, particular user(s), and particular protected information. (5) Each **Component Assembly** is independently assembled, loadable and deliverable vis-à-vis other **Component Assemblies**. (6) The dynamic assembly of a **Component Assembly** is directed by a "blueprint" *Record* **Containing** control information for this particular activity on this particular information by this particular user(s). (7) **Component Assemblies** are extensible and can be configured and reconfigured (modified) by all users, and combined by all users with other **Component Assemblies**, subject only to other users' "senior" **Controls**. For the purposes of the construction of "Component Assembly," "*Load Module*," "*Secure Processing Environment*" and "*Record*" are defined as set forth in item #4 above.
100.	at least one of said elements including at least some	executable programming (executable): see item #73 above	executable programming: A cohesive series of machine code instructions, comprising a computer program, in a

	'912 Claim 8	IT Construction	MS Construction
	executable programming,		format that can be loaded into memory and run (executed) by a connected processor. A "computer program" is a complete series of definitions and instructions that when executed on a computer will perform a required or requested task.
101.	at least one of said elements constituting a load module,		
102.	said load module including **executable programming** and a header;	executable programming (executable): see item #73 above	executable programming: see item #100 above
103.	said header including an execution space **identifier** *identifying at least one aspect of an execution space required for use and/or execution of the load module* associated with said header;	identifier: see item #28 aspect: see item #59 above use: see item #42 above identifying at least one aspect of an execution space required for use and/or execution of the load module: Normal English, incorporating the separately defined terms: identifying an Aspect (e.g. security level) of an execution space that is needed in order for the load module to execute or otherwise be used.	identifier: see item #28 aspect: see item #59 above use: see item #42 above identifying at least one aspect of an execution space required for use and/or execution of the load module: (1) Defining fully, without reference to any other information, at least one of the persistent elements or properties (**Aspects**) (that are capable of being used to distinguish it from other environments of an execution space) that are required for any **Use**, and/or for any execution, of the *Load Module*. (2) An execution space without all of those required aspects is incapable of making any such execution and/or other **Use** (e.g., **Copying**, displaying, printing) of the *Load Module*. For the purposes of the construction of this phrase, a "*Load Module*" is defined as set forth in item #4, above

	'912 Claim 8	IT Construction	MS Construction
104.	said execution space **identifier** provides the capability for distinguishing between execution spaces providing a higher level of security and execution spaces providing a lower level of security;	identifier: see item #28	identifier: see item #28
105.	using said information to identify and locate said one or more elements;		
106.	accessing said located one or more elements;		
107.	**securely** assembling said one or more elements to form at least a portion of said first **component assembly;**	securely: see item #3 above component assembly: see item #98 above	securely: see item #3 above component assembly: see item #98 above
108.	executing at least some of said **executable programming**; and	executable programming (executable): see item #73 above	executable programming: see item #100 above
109.	checking said record for validity prior to performing said executing step.		

U.S. Patent No. 5,917,912, Asserted Claim 35

	'912 Claim 35	IT Construction	MS Construction
110.	35. A process comprising the following steps:	The claim contains no requirement of a VDE.	Claim as a whole: The recited method is performed within a **VDE.** (See item #86 for Microsoft's construction of **VDE.**)
111.	at a first processing environment receiving a first record from a second processing environment remote from said first processing environment;		
112.	said first record being received in a **secure container;**	secure container: see item #57 above	secure container: see item #57 above
113.	said first record **containing** identification information directly or indirectly identifying one or more elements of a first **component assembly;**	containing: see item #57 above component assembly: see item #98 above	containing: see item #57 above component assembly: see item #98 above
114.	at least one of said elements including at least some **executable programming;**	executable programming (executable): see item #73 above	executable programming: see item #100 above
115.	said **component assembly** allowing access to or **use** of specified information;	component assembly: see item #98 above use: see item #42 above	component assembly: see item #98 above use: see item #42 above
116.	said **secure container** also including a first of said elements;	secure container: see item #57 above	secure container: see item #57 above
117.	accessing said first record;		
118.	using said identification information to identify and locate		

	'912 Claim 35	IT Construction	MS Construction
	said one or more elements;		
119.	said locating step including locating a second of said elements at a third processing environment located remotely from said first processing environment and said second processing environment;		
120.	accessing said located one or more elements;		
121.	said element accessing step including retrieving said second element from said third processing environment;		
122.	**securely** assembling said one or more elements to form at least a portion of said first **component assembly** specified by said first record; and	securely (secure): see item #3 above component assembly: see item #98 above	securely (secure): see item #3 above component assembly: see item #98 above
123.	executing at least some of said **executable programming,**	executable programming (executable): see item #73 above	executable programming: see item #100 above
124.	said executing step taking place at said first processing environment.		